Abstract

A secure method for changing a password to a new password when the passwords are being transmitted over a network is presented. The present invention does not require the use of any additional keys (such as symmetric keys or public/private key pairs) to protect the password exchanges. Moreover, the present solution does not require the use of any encryption algorithms (such as DES, RC4/RC5, etc.), it only requires the use of a collision-resistant hash function.